

Security of Power Packet Dispatching Using Differential Chaos Shift Keying

Yanzi Zhou,^{*} Ryo Takahashi,[†] and Takashi Hikihara[‡]

Department of Electrical Engineering, Kyoto University, Katsura, Nishikyo, Kyoto, 615-8510 Japan
(Dated: March 10, 2015)

This paper investigates and confirms one advantageous function of a power packet dispatching system, which has been proposed by authors' group with being apart from the conventional power distribution system. Here is focused on the function to establish the security of power packet dispatching for prohibiting not only information but also power of power packet from being stolen by attackers. For the purpose of protecting power packets, we introduce a simple encryption of power packets before sending them. Encryption scheme based on chaotic signal is one possibility for this purpose. This paper adopts the Differential Chaos Shift Keying (DCSK) scheme for the encryption, those are partial power packet encryption and whole power packet encryption.

INTRODUCTION

In the context of the growth of renewable power sources in electricity generation, a novel power packet dispatching system has been proposed for the purpose of managing low power renewable power sources together with commercial power sources and supplying power based on demands [1–4]. The basic configuration of the power packet dispatching system, which consists of DC power sources, a mixer, power line, a router, and loads, is illustrated in Fig. 1. The mixer produces power packets by switching selected power sources on and off based on its clock frequency. The proposed configuration of one power packet is presented in Fig. 2, which includes information tags and payload [5]. In particular, useful information, such as the power source and power destination (load address), are the main part of the header. The footer is the end signal of one power packet and the payload carries electric power. Power packets are transmitted from a mixer to a router through a power line in the Time-Division Multiplexing (TDM) fashion. The router is in charge of determining the route for each power packet according to the information attached in the header and transferring power to the requested load [2, 6, 7]. For the sake of recognition of the packet signal in the router so as to determine the route for power packets precisely, the clock synchronization between the mixer and router is required. Different clock synchronization methods have been employed in the power packet dispatching system. In [6] the clock synchronization has been achieved by a clock recovery circuit and in [8] an external clock line is adopted for external synchronization. However, the line connection for synchronization limits the extension of system distribution, because of the delay and noise generated by clock lines. The failure in synchronization caused by the deficiency of external clock line is explained theoretically in [9]. In [10], a first order control of digital clock synchronization is applied and the clock synchronization is achieved automatically between the mixer and router with the aid of the preamble of power packet. The preamble contains several cycles of the mixer clock signal. The performance of clock synchronization is improved by

a second order control scheme in [5].

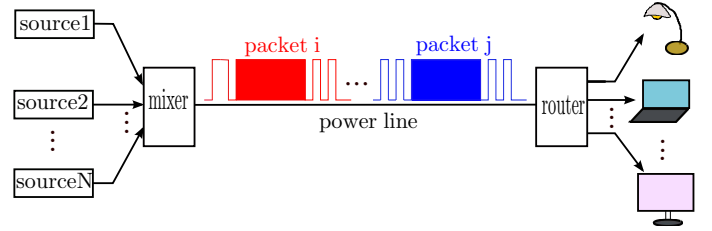


FIG. 1: Basic configuration of power packet dispatching system. Power packets are generated in the mixer and transmitted to the router. The power contained in each power packet is dispatched to the load designated by the information tags of the power packet.

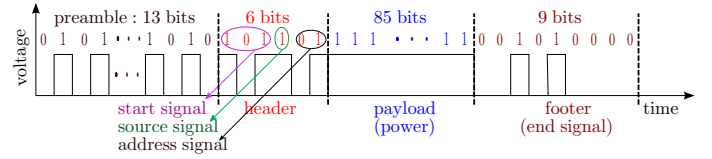


FIG. 2: Basic composition of one power packet. The preamble is several cycles of mixer clock signal used to achieve the clock synchronization, the header includes useful information, the payload carries power and the footer indicates the end of one power packet.

The security of power packet dispatching is defined as protecting the content of power packet, which consists of both information tags and power, from unknown consumer (attacker). For the system in Fig. 1, when an attacker who exists between the mixer and the router receives power packets, he may deduce the packet signal and then obtain private information of consumers. With respect to power, the attacker can steal the power if he connects some devices directly to the power line. In other words, there is no security in the basic power packet dispatching system according to the definition of security. We can easily imagine that the attacker may even change the information purposely and then send the tampered packet to the router. In doing so, he may give rise to wrong power dispatching, which will possibly

cause a damage to the running system. Considering the consumers' privacy and safety of the system, the security of power packet between the mixer and router should be established. For this purpose, we propose to encrypt power packets before sending them.

Spread spectrum communications have been widely used in secure communication field. The uniform spreading of spectrum is one of the desired features in encryption. This is because the spectrum may be one of the clues for decryption. Besides that, a message may be hidden in the background noise by spreading its bandwidth with coding and by transmitting signal at a low averaged power, which is called a low-probability-of-intercept [11]. Chaotic sequences are very appealing for the use as carriers in Direct-Sequence Spread Spectrum (DSSS) system due to their broad band spectrum. They can spread spectrum more uniformly compared with the conventional sequences such as the Gold sequence and Walsh-Hadamard sequence as described in [12]. Power spread is also considered in [13, 14]. The possibility of synchronization between chaotic systems was reported by Pecora and Carroll [15–17]. After that, many chaos-based communication systems had been proposed and analyzed [12, 18–31]. In the power packet dispatching system, power packet is generated in digital form. Hence, digital encryption scheme is required. Chaos Shift Keying (CSK) scheme with coherent detection was firstly proposed in [18, 20] to encode digital symbols with chaotic signals. However, the sensitive dependence of chaotic signals upon initial condition makes it very difficult to replica signal in the receiver [25]. Therefore, in chaos-based communication systems, non-coherent detection of received signal has advantage over coherent detection. The Differential Chaos Shift Keying (DCSK) scheme is a typical non-coherent chaos-based communication scheme [22], which also solves the problem of threshold shift in non-coherent CSK system [25]. In view of features of the DCSK scheme, we investigate the power packet encryption using DCSK scheme to establish the security of power packet dispatching in this paper.

The rest of the paper is organized as follows. In Section 2, the operating principles of DCSK scheme are summarized according to references [22, 25] for its application to power packet encryption. Section 3 presents two power packet encryption methods using DCSK scheme, which are partial power packet encryption and whole power packet encryption. At the same time, the security status of power packet is also discussed. Power transfer through the modulator is analyzed and then examined through simulations in Section 4. The final section is devoted for the conclusions.

DIFFERENTIAL CHAOS SHIFT KEYING

The operating principles of the Differential Chaos Shift Keying (DCSK) scheme was reported in [22, 25]. Figure 3(a) presents the block diagram of a DCSK modulator. In the scheme, every information bit period is divided into two equal time slots, so that every bit b_l can be represented by two consecutive chaotic sequences: reference sequence and data sequence. Here, $l \in \mathbb{N}_1$ denotes the serial number of information bits. In the first half bit period, the chaotic signal x_k is transmitted ($k \in \mathbb{N}_1$ indicates the serial number of sample points of the chaotic signal). During the second half bit period the data sequence is transmitted. The data sequence is determined by b_l and the reference sequence. When the information bit to be sent is '1', the data sequence is identical to the reference sequence. Whereas, if the information bit is '-1', the data sequence is inverted to the reference sequence. In this way, the data sequence carries information bits. The representation of one information bit b_1 using DCSK scheme is exemplified in Fig. 4. Let T_b and T_x represent the information bit period and the time interval between two adjacent points of chaotic signal, respectively. The relationship of T_b and T_x is given as

$$T_b = 2\beta T_x, \quad (1)$$

where 2β is referred to as the spreading factor in the DCSK scheme ($\beta \in \mathbb{N}_1$). Consequently, the data sequence can be represented as $\{\pm x_{k-\beta}\}$, $k = \beta + 1, \beta + 2, \dots, 2\beta$ for $l = 1$. The output signal of the DCSK modulator s_k , i.e., the transmitted signal, during the l -th bit period can be given as follows for $b_l = '1'$,

$$s_k = \begin{cases} x_k, & (l-1)2\beta + 1 \leq k \leq (l-1)2\beta + \beta, \\ x_{k-\beta}, & (l-1)2\beta + \beta + 1 \leq k \leq (l-1)2\beta + 2\beta. \end{cases} \quad (2)$$

When a '-1' is sent, s_k can be expressed in a likewise fashion,

$$s_k = \begin{cases} x_k, & (l-1)2\beta + 1 \leq k \leq (l-1)2\beta + \beta, \\ -x_{k-\beta}, & (l-1)2\beta + \beta + 1 \leq k \leq (l-1)2\beta + 2\beta. \end{cases} \quad (3)$$

The block diagram of a DCSK demodulator [25] is presented in Fig. 3(b). The output of the correlator y_l can be obtained at the end of the l -th bit period by the following equation.

$$y_l = \sum_{k=(l-1)2\beta+\beta+1}^{(l-1)2\beta+2\beta} r_k r_{k-\beta}. \quad (4)$$

Comparing y_l with the threshold value of the threshold detector, the information bit can be recovered at the output of the demodulator as b'_l . Suppose that the transmitted signal s_k passes through an Additive White Gaussian

Noise (AWGN) channel [25]. The received signal r_k can be given as

$$r_k = s_k + \xi_k, \quad (5)$$

where ξ_k represents the k -th sampling point of the white Gaussian noise which is assumed to be of zero mean and variance as $N_0/2$. If a '+1' is transmitted, s_k is as in Eq. (2). Substituting Eqs. (2) and (5) into Eq. (4), y_l can be described in more detail as follows.

$$\begin{aligned} y_l &= \sum_{k=(l-1)2\beta+1}^{(l-1)2\beta+2\beta} r_k r_{k-\beta} \\ &= \sum_{k=(l-1)2\beta+1}^{(l-1)2\beta+\beta} r_{k+\beta} r_k \\ &= \sum_{k=(l-1)2\beta+1}^{(l-1)2\beta+\beta} (s_{k+\beta} + \xi_{k+\beta})(s_k + \xi_k) \\ &= \sum_{k=(l-1)2\beta+1}^{(l-1)2\beta+\beta} (x_k + \xi_{k+\beta})(x_k + \xi_k) \\ &= \sum_{k=(l-1)2\beta+1}^{(l-1)2\beta+\beta} x_k^2 + \sum_{k=(l-1)2\beta+1}^{(l-1)2\beta+\beta} x_k(\xi_k \\ &\quad + \xi_{k+\beta}) + \sum_{k=(l-1)2\beta+1}^{(l-1)2\beta+\beta} \xi_k \xi_{k+\beta}. \end{aligned} \quad (6)$$

Let $\sum_{k=(l-1)2\beta+1}^{(l-1)2\beta+\beta} x_k^2$, $\sum_{k=(l-1)2\beta+1}^{(l-1)2\beta+\beta} x_k(\xi_k + \xi_{k+\beta})$, and $\sum_{k=(l-1)2\beta+1}^{(l-1)2\beta+\beta} \xi_k \xi_{k+\beta}$ be denoted by A , B , and C , respectively. A is related only to the chaotic signal x_k and is positive. B and C are noise interference. However, if a '-1' is sent, s_k is as in Eq. (3). Accordingly, y_l becomes

$$\begin{aligned} y_l &= \sum_{k=(l-1)2\beta+1}^{(l-1)2\beta+\beta} (-x_k^2) + \sum_{k=(l-1)2\beta+1}^{(l-1)2\beta+\beta} [-x_k(\xi_k + \xi_{k+\beta})] \\ &\quad + \sum_{k=(l-1)2\beta+1}^{(l-1)2\beta+\beta} \xi_k \xi_{k+\beta}. \end{aligned} \quad (7)$$

Let $\sum_{k=(l-1)2\beta+1}^{(l-1)2\beta+\beta} (-x_k^2)$ and $\sum_{k=(l-1)2\beta+1}^{(l-1)2\beta+\beta} [-x_k(\xi_k + \xi_{k+\beta})]$ be denoted by A' and B' , respectively. A' is also related only to the chaotic signal x_k but it is negative. Since AWGN channel is assumed between the modulator and demodulator, it can be deduced that both B (or B') and C have a zero mean. Therefore, the threshold value of the detector can be set at zero optimally. As a consequence,

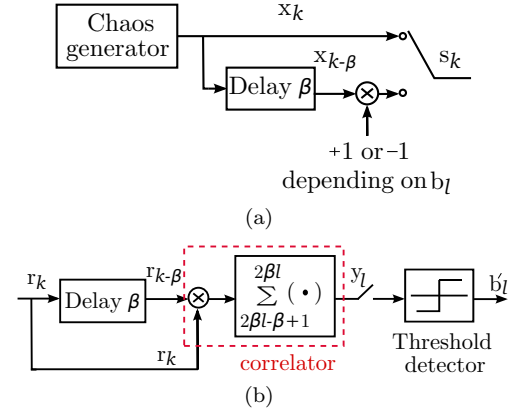


FIG. 3: Block diagram of a non-coherent single-user DCSK system. (a) modulator; x_k and $x_{k-\beta}$ are chaotic signal and its half-bit (β) delayed version, respectively. They are used to represent the information bit b_l . s_k is the modulator output. (b) demodulator. r_k and $r_{k-\beta}$ are received signal and its half-bit delayed version, respectively. y_l is the convolution of r_k and $r_{k-\beta}$ during the l -th bit period while b'_l is the recovered l -th information bit. 2β is the spreading factor in the DCSK scheme.

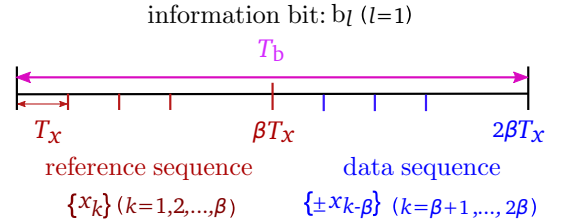


FIG. 4: Representation of one information bit b_1 using DCSK scheme. The information bit period T_b is divided into two equal time slots. b_1 is represented by two consecutive chaotic sequence: reference sequence and data sequence ($\{x_k\}$ and $\{\pm x_{k-\beta}\}$). The sign of data sequence is determined by b_1 (if $b_1 = '1'$, the data sequence is $\{x_{k-\beta}\}$, otherwise, it is $\{-x_{k-\beta}\}$). T_x indicates the time interval between two adjacent points of chaotic sequence ($T_b = 2\beta T_x$).

the information bit can be recovered through the detector as

$$b'_l = \begin{cases} '+1', & y_l > 0, \\ '-1', & y_l < 0. \end{cases} \quad (8)$$

POWER PACKET ENCRYPTION

Given the principles of DCSK scheme in section , we apply the scheme to encrypt power packet aiming to establish the security of power packet dispatching. When the scheme is applied to power packet encryption, the packet signals are encrypted as information bits in a conventional DCSK modulator. In this section, two en-

ryption methods for power packet will be discussed, i.e., partial power packet encryption and whole power packet encryption. From the principle of DCSK demodulator, the spreading factor (2β) should be obtained by the demodulator in advance so that the information bits can be recovered correctly. We refer to 2β as key in our encryption methods.

Partial Power Packet Encryption

In the power packet dispatching system, the synchronization is essential to handshake between the sender and receiver of power packet, that is, the mixer and router. As shown in Fig. 2, the preamble is designed for achieving the clock synchronization between the mixer and router [10]. At the meantime, from the viewpoint of privacy protect, the header should be hidden during transmission, because the header may include consumers' private information. Therefore the security of information is possibly established, provided that the preamble and header are protected. In partial power packet encryption, only preamble and header are encrypted using DCSK scheme. The rest of the packet (payload and footer) remains unencrypted. The encryption method is illustrated in Fig. 5. The mixer is integrated with a DCSK modulator and the router is integrated with a DCSK demodulator. As shown in this figure, the power packet generated by the mixer is partially encrypted through the DCSK modulator. The encrypted packet is then transmitted. In demodulator, the encrypted packet can be recovered if the key is obtained beforehand as mentioned in section . The whole packet can be recovered, not only because the recovered preamble and header suffice to determine the route of power packet in the router, but also based on the fact that the unencryption of the payload and footer guarantees the power in power packet.

Under partial encryption, assume that an attacker exists in the system during power packet transmission. The security status of information and power can be analyzed. Here, we focus on the information contained in the preamble and header without considering the footer, since the footer is the end signal of a power packet. When the packet is caught by the attacker, he can not obtain information because of the disability of recovering the packet signals without the key. Therefore, the security of information is achieved. Nevertheless, the power can be stolen by the attacker if he connect some device directly to the power line. It means the security of power can not be achieved in this method. In addition, the power of power packet is carried by the payload as mentioned in section . Therefore, whole power of packet may be stolen by the attacker since the payload is transmitted without encryption.

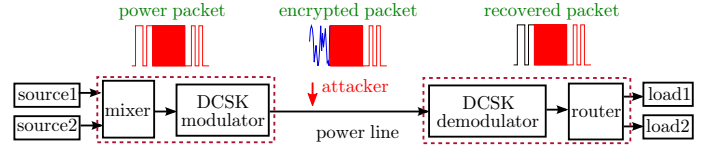


FIG. 5: Diagram of system with partial power packet encryption. The power packet is partially encrypted by the DCSK modulator. The encrypted packet is recovered through the demodulator before it arrives to the router. Finally, the power contained in the power packet is delivered to the desired load.

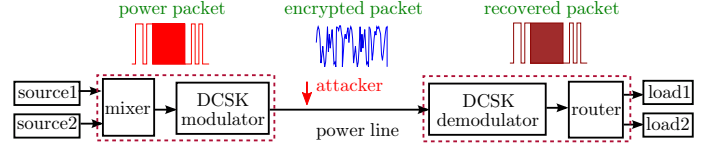


FIG. 6: Diagram of system with whole power packet encryption. The whole power packet is encrypted by the DCSK modulator. The encrypted packet is recovered through the demodulator before it arrives to the router. Finally, the power contained in the power packet is delivered to the desired load.

Whole Power Packet Encryption

In order to further improve the security of power packet dispatching, we propose to encrypt the whole power packet. Figure 6 shows the whole power packet encryption method. It is clear that there is no difference in the security of information between these two methods, since the preamble and header are encrypted in both methods. Next, we will discuss about the power. The power can still be stolen by the attacker if he connects some devices directly to the power line. However, we should bear in mind that payload carries the power of packet. Thus what calls for special attention is that once the payload is encrypted, the power of encrypted packet may be changed.

The whole encryption method encrypts both information tags and payload. It is different from the original DCSK scheme, where the transferred signal is digital data without physical quantity. In order to transfer power, the DCSK modulator is modified as in Fig. 7. In the chaos generator, we suppose the generated chaotic signal carries power for encryption. The data sequence becomes the product of chaotic signal and the packet signal. The voltage amplitude of packet signal is '+a' or '-a' in volts. Let the payload consists of N_b bits packet signal. Then the average output power of modulator P_{modout} in watts (W) can be calculated during payload according to

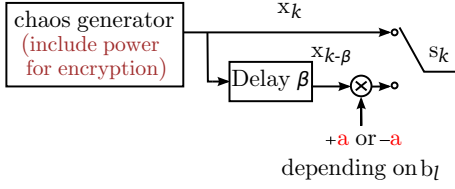


FIG. 7: Block diagram of modulator used in whole power packet encryption. This is the modified version of the original DCSK modulator. a is the absolute voltage amplitude of the packet signal b_l .

Eq. (2) with replacing $x_{k-\beta}$ by $ax_{k-\beta}$ as follows:

$$P_{\text{modout}} = \frac{\sum_{l=1}^{N_b} \left(\sum_{m=1}^{\beta} x_{lm}^2 T_x + \sum_{m=1}^{\beta} a^2 x_{lm}^2 T_x \right)}{N_b T_b} \quad (9)$$

$$= \frac{(1 + a^2) \sum_{l=1}^{N_b} \sum_{m=1}^{\beta} x_{lm}^2}{2\beta N_b},$$

where x_{lm} denotes the m -th sample point of chaotic signal in the first half bit period of the l -th bit packet signal. Equation (9) shows the possibility of rescaling the output power of modulator P_{modout} by the voltage amplitude of packet signal a , the spreading factor 2β , the bit number of packet signal during payload N_b and chaotic signal. From the viewpoint of the amount of stolen power, we say that the power of power packet under whole encryption becomes more secure compared to the partial encryption method.

We consider the original power packet is the input of the modulator and thus the average input power of the modulator during payload is a^2 in watts, since the voltage of packet signal is constant at a V throughout the payload. Power efficiency of the modulator η_{mod} is defined as below,

$$\eta_{\text{mod}} = \frac{(1 + a^2) \sum_{l=1}^{N_b} \sum_{m=1}^{\beta} x_{lm}^2}{2\beta N_b a^2}. \quad (10)$$

It corresponds to the ratio of the output power divided by the input power of the modulator. η_{mod} is possible to rescale by a , 2β , N_b , and x_k . As a result, the range of input power can be expanded to meet the demand of power from loads. This might be another benefit of whole packet encryption using DCSK scheme.

SIMULATION RESULTS OF TRANSFERRED POWER

In order to confirm the power transferred through DCSK modulator in whole encryption case, we build a model of DCSK modulator in Simulink. In simulations, the power packet shown in Fig. 2 is adopted. From

Eq. (9), the power spectrum of s_k is related to the chaotic signal. Hence we begin with introduction of the chaotic signal utilized in simulations for analyzing the average power of s_k in payload duration.

In simulations, the chaotic signal x_k is produced by the following normalized improved logistic map [25],

$$x_{k+1} = \sqrt{2}(1 - x_k^2). \quad (11)$$

The sensitive dependence upon initial conditions of the produced chaotic signal is presented in Fig. 8. Both $c1$ and $c2$ in Fig. 8 are produced by Eq. (11) but with different initial conditions as $c1(1)=0.75$ and $c2(1)=0.749$. Next, the auto-correlation function of x_k ($R_{xx}[n]$) is de-

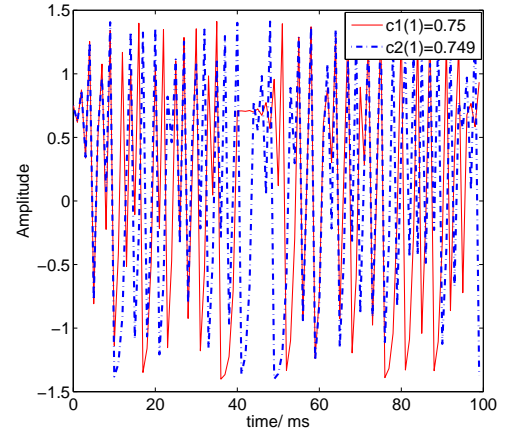


FIG. 8: Waveforms of chaotic signals generated by iterative map $x_{k+1} = \sqrt{2}(1 - x_k^2)$ with different initial values. $c1(1)=0.75$, $c2(1)=0.749$. The time interval between signals is $T_{c1} = T_{c2} = 0.001$ s and the simulation time is 0.1 s, which implies the length of signals plotted here is $N_{c1} = N_{c2} = 100$.

fined as

$$R_{xx}[n] = E(x_k x_{k-n}), \quad (12)$$

where n represents the time-lag and $E(\cdot)$ is the expected value operator. The power spectral density function is the Fourier transform of the auto-correlation function. Shown in Figs. 9 and 10 are the numerical approximations of the auto-correlation function and power spectral density of x_k using finite-length ($N_x = 1000$) signals, respectively. Figure 9 indicates x_k is almost random. The power spectral density in Fig. 10 shows the wide-band property of x_k , which implies the aperiodicity.

As mentioned above, the power packet in [5] is employed, thus $N_b = 85$. We set the initial value of the chaotic signal x_1 at 0.75 without loss of generality. According to Eq. (11), x_k is limited in the range of $[-1.4142, +1.4142]$. In addition, if the bit length of packet signal T_b is determined, then the values of x_k during payload can be obtained. The dependency of the output power of modulator P_{modout} on a and 2β can be

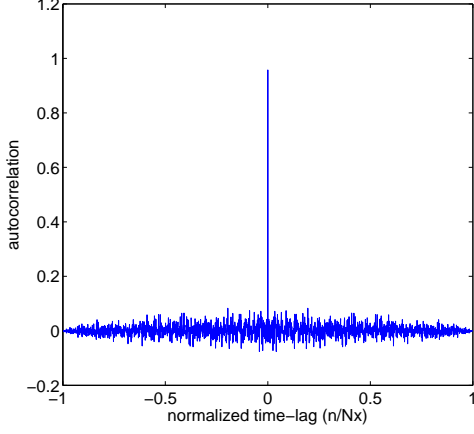


FIG. 9: Normalized approximated auto-correlation of x_k , which is generated by iterative map $x_{k+1} = \sqrt{2}(1 - x_k^2)$ with $x_1 = 0.75$ and the time step is $T_x = 0.001$ s. The generated samples are of finite length 1000.

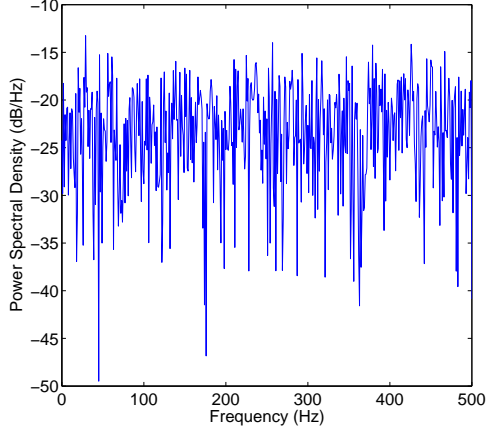


FIG. 10: Approximated power spectral density of x_k , which is generated by the iterative map $x_{k+1} = \sqrt{2}(1 - x_k^2)$ with $x_1 = 0.75$ and time step is $T_x = 0.001$ s. The generated samples are of finite length 1000.

examined in simulations. We set $T_x = T_{\text{sam}} = 0.001$ s without loss of generality. T_{sam} represents the sampling period in simulations.

When we fix $2\beta = 100$, the power spectrums of s_k with different values of a ($a = 1$, $a = 2$, $a = 5$, and $a = 10$) are obtained as shown in Fig. 11. The magenta lines in these figures show the average power of s_k , which means P_{modout} . We refer to the value of P_{modout} obtained from the power spectrum of s_k through simulations as $P_{\text{modoutsim}}$, as given in Table I. The mean values of x_k and x_k^2 are $E[x_k] = 0.0018$ and $E[x_k^2] = 1.0067$ at $T_{\text{sam}} = 0.001$ s and $2\beta = 100$. Then P_{modout} can be numerically calculated by Eq. (9) as in Table I. In Table I, with the increase of a , P_{modout} tends to be half of the

input power a^2 . This can be explained by substituting $E[x_k^2] = 1.0067$ into Eq. (10).

TABLE I: Power transferred through modulator with different values of a while 2β is fixed at 100. $P_{\text{modoutsim}}$ and P_{modout} corresponds to simulation result and calculation result, respectively.

a/V	1	2	5	10
$P_{\text{modoutsim}}/W$	1.007	2.517	13.09	50.84
P_{modout}/W	1.0067	2.51675	13.0871	50.83835

Keeping $a = 2$ the power spectrum of s_k is considered for 2β ($2\beta = 50, 100, 500$, and 1000). The power spectrums are obtained as in Fig. 12. Similarly, $P_{\text{modoutsim}}$ are listed in Table III. $E[x_k^2]$ is obtained through iteration as in Table II. $E[x_k^2]$ are different because the number of samples varies with 2β . However, the difference is small due to the random feature of chaotic signal. Then P_{modout} with different 2β can also be calculated according to Eq. (9), as given in Table III. We can see that P_{modout} almost keep the same with the change of 2β . It can be explained by Eq. (9) and Table II. According to Eq. (9), P_{modout} depends only on $E[x_k^2]$ when a , 2β , and N_b are known. According to Table II, the values of $E[x_k^2]$ with different 2β changes little, and thus P_{modout} are almost the same.

TABLE II: Mean values of x_k^2 ($E[x_k^2]$) during payload with different values of 2β while a is fixed at 2.

2β	50	100	500	10000
$E[x_k^2]$	1.0065	1.0067	1.0046	0.9996

TABLE III: Power transferred through modulator with different values of 2β while a is fixed at 2. $P_{\text{modoutsim}}$ and P_{modout} corresponds to simulation result and calculation result, respectively.

2β	50	100	500	1000
P_{spay}/W	2.516	2.517	2.512	2.499
P_{modout}/W	2.51625	2.51675	2.5115	2.499

CONCLUSIONS

In this paper, we proposed to encrypt power packets before sending them in a power packet dispatching system for the purpose of protecting the content of power packets. At first, we summarized the principles of the DCSK scheme referring to other researchers' work. Then partial power packet encryption method using DCSK scheme was proposed. The security of information and

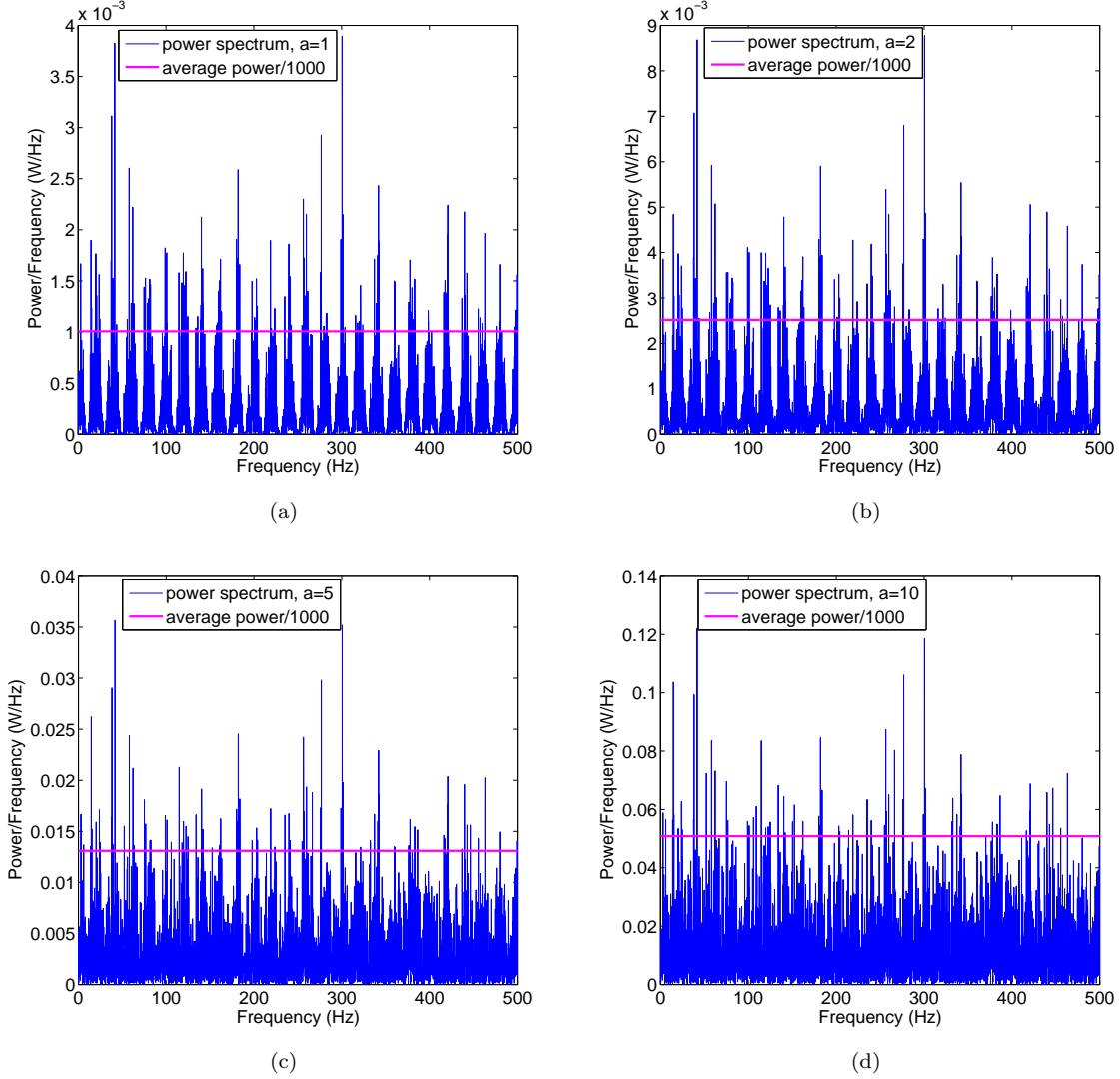


FIG. 11: Power spectrum of DCSK modulator output signal s_k in simulations with different values of a , while $T_{\text{sam}} = 0.001$ s and $2\beta = 100$. The data is limited in payload duration. T_{sam} is the sampling period in simulations, 2β the spreading factor and a the absolute amplitude of packet signal in volts. (a) $a = 1$; (b) $a = 2$; (c) $a = 5$; (d) $a = 10$. The magenta line represents the value of average power of s_k in payload duration.

power of packet were discussed, separately. Next, we proposed to encrypt the whole power packet in order to further improve the security. The power of encrypted power packet was then examined in simulations.

Applying power packet encryption, the information of packet is protected from attackers. The power is protected in a certain extent from the viewpoint of the amount of stolen power. In addition, due to the principles of DCSK scheme, the power of packet after whole encryption can be rescaled. This might be a potential advantage to expand the range of power sources to meet the demand of loads.

This work was supported by Council for Science, Technology and Innovation (CSTI), Cross-ministerial

Strategic Innovation Promotion Program (SIP), “Next-generation power electronics” (funding agency: NEDO). The authors also acknowledge to Prof. Ken Umeno and Prof. Yasuo Okabe for fruitful discussions. The author (R.T.) was partially supported by the JSPS, Grant-in-Aid for Young Scientist (B), 26820144.

REFERENCES

* Electronic address: y-zhou@dove.kuee.kyoto-u.ac.jp

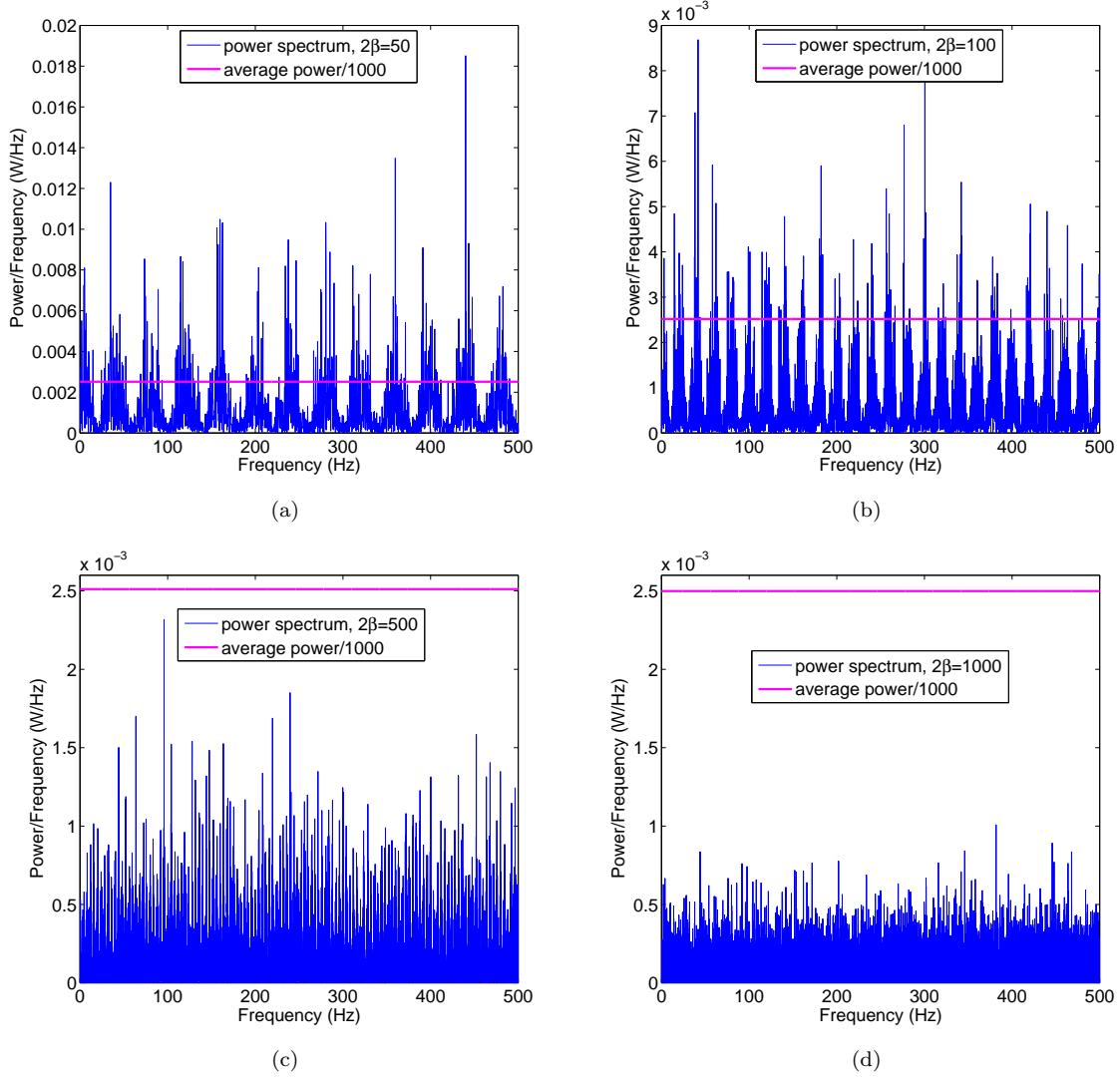


FIG. 12: Power spectrum of DCSK modulator output s_k in simulation with different values of 2β , while $T_{\text{sam}} = 0.001$ s and $a = 2$. The data is limited in payload duration. T_{sam} is the sampling period in simulations, 2β the spreading factor and a the absolute amplitude of packet signal in volts. (a) $2\beta = 50$; (b) $2\beta = 100$; (c) $2\beta = 500$; (d) $2\beta = 1000$.

[†] Electronic address: takahashi.ryo.2n@kyoto-u.ac.jp

[‡] Electronic address: hikiyara.takashi.2n@kyoto-u.ac.jp

- [1] T. Hikiyara, "Power router and packetization project for home electric energy management," *Proc. Santa Barbara Summit on Energy Efficiency*, Santa Barbara, CA, USA, pp. 12–13, 2010.
- [2] T. Takuno, M. Koyama, and T. Hikiyara, "In-home power distribution systems by circuit switching and power packet dispatching," *Proc. First IEEE International Conference on SmartGridComm*, pp. 427–430, IEEE, 2010.
- [3] T. Takuno, Y. Kitamori, R. Takahashi, and T. Hikiyara, "AC power routing system in home based on demand and supply utilizing distributed power sources," *Energies*, vol. 4, no. 5, pp. 717–726, 2011.
- [4] R. Takahashi, T. Takuno, and T. Hikiyara, "Estimation

of power packet transfer properties on indoor power line channel," *Energies*, vol. 5, no. 7, pp. 2141–2149, 2012.

- [5] Y.Z. Zhou, R. Takahashi, and T. Hikiyara, "Power Packet Dispatching with Second-Order Clock Synchronization," *International Journal of Circuit Theory and Applications*, submitted, 2014.
- [6] K. Tashiro, R. Takahashi, and T. Hikiyara, "Feasibility of power packet dispatching at in-home dc distribution network," *Proc. Third IEEE International Conference on SmartGridComm*, pp. 401–405, IEEE, 2012.
- [7] R. Takahashi, K. Tashiro, and T. Hikiyara, "Router for Power Packet Distribution Network: Design and Experimental Verification," *IEEE Trans. Smart Grid*, 2015, in press.
- [8] N. Fujii, R. Takahashi, and T. Hikiyara, "Networked Power Packet Dispatching System for Multi-path Routing," *Proc. IEEE/SICE International Symposium on*

- System Integration*, pp. 357–362, IEEE, 2014.
- [9] S. Nawata, N. Fujii, Y.Z. Zhou, R. Takahashi, and T. Hikiyara, “A theoretical examination of an unexpected transfer of power packets by synchronization failure,” *Proc. NOLTA*, pp. 60–63, IEICE, 2014.
 - [10] Y.Z. Zhou, R. Takahashi, and T. Hikiyara, “Realization of Autonomous Clock Synchronization for Power Packet Dispatching,” *IEICE Trans. Fundamentals*, vol. E98-A, no. 2, 2015, in press.
 - [11] J.G. Proakis and M. Salehi, *Digital Communications(fifth edition)*, McGraw-Hill Education, 2007.
 - [12] R. Takahashi and K. Umeno, “Performance Evaluation of CDMA Using Chaotic Spreading Sequence with Constant Power in Indoor Power Line Fading Channels,” *IEICE Trans. Fundamentals*, vol. E97-A, no. 7, pp. 1619–1622, 2014.
 - [13] D.C. Hamill, J.H. Deane, and P.J. Aston, “Some applications of chaos in power converters,” *IEE Colloquium: Update on New Power Electronic Techniques*, Digest No: 1997/091, 1997.
 - [14] A. Kordonis and T. Hikiyara, “Harmonic Reduction and Chaotic Operation towards Application of AC/AC Converter with Feedback Control,” *IEICE Trans. Fundamentals*, vol. 97, no. 3, pp. 840–847, 2014.
 - [15] L.M. Pecora and T.L. Carroll, “Synchronization in chaotic systems,” *Phys. Rev. Lett.*, vol. 64, no. 8, pp. 821–824, 1990.
 - [16] L.M. Pecora and T.L. Carroll, “Driving systems with chaotic signals,” *Phys. Rev. A*, vol. 44, no. 4, pp. 2374–2383, 1991.
 - [17] T.L. Carroll, and L.M. Pecora, “Synchronizing chaotic circuits,” *IEEE Trans. Circuits Syst.*, vol. 38, no. 4, pp. 453–456, April, 1991.
 - [18] U. Parlitz, L.O. Chua, L. Kocarev, K.S. Halle, and A. Shang, “Transmission of digital signals by chaotic synchronization,” *International Journal of Bifurcation and Chaos*, vol. 2, no. 4, pp. 973–977, 1992.
 - [19] K.M. Cuomo and A.V. Oppenheim, “Circuit implementation of synchronized chaos with applications to communications,” *Phys. Rev. Lett.*, vol. 71, no. 1, pp. 65–68, 1993.
 - [20] H. Dedieu, M. Kennedy, P. Michael, and M. Hasler, “Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua’s circuits,” *IEEE Trans. Circuits Syst. II*, vol. 40, no. 10, pp. 634–642, 1993.
 - [21] T. Kohda and A. Tsuneda, “Pseudonoise sequences by chaotic non-linear maps and their correlation properties,” *IEICE Trans. Commun.*, vol. E76-B, no. 8, pp. 855–862, August 1993.
 - [22] G. Kolumban, “Differential chaos shift keying: A robust coding for chaotic communication,” *Proc. 4th Int. Workshop on NDES*, pp. 87–92, 1996.
 - [23] Y. Tao, C.W. Wu, and L.O. Chua, “Cryptography based on chaotic systems,” *IEEE Trans. Circuits Syst. I*, vol. 44, no. 5, pp. 469–472, 1997.
 - [24] G. Kolumban, M.P. Kennedy, Z. Jako, and G. Kis, “Chaotic communications with correlator receivers: theory and performance limits,” *Proc. IEEE*, vol. 90, no. 5, pp. 711–732, May, 2002.
 - [25] F.C.M. Lau and C.K. Tse, “Performance Analysis Methods for Non-Coherent Differential Chaos-Shift-Keying Systems,” in *Chaos-Based Digital Communication Systems*, pp. 63–96, Springer Berlin Heidelberg, 2003.
 - [26] Y. Tao, “A survey of chaotic secure communication systems,” *International Journal of Computational Cognition*, vol. 2, no. 2, pp. 81–130, 2004.
 - [27] H. Chen, J. Feng, and C.K. Tse, “A general noncoherent chaos-shift-keying communication system and its performance analysis,” *Proc. ISCAS 2007.*, pp. 2466–2469, IEEE, 2007.
 - [28] SG. Stavriniades, AN. Anagnostopoulos, AN. Miliou, A. Valaristos, L. Magafas, K. Kosmatopoulos, and S. Papaioannou, “Digital chaotic synchronized communication system,” *J. Eng. Sci. Technol. Rev.*, vol. 2, no. 1, pp. 82–86, 2009.
 - [29] R. Takahashi and K. Umeno, “Performance analysis of complex CDMA using complex chaotic spreading sequence with constant power,” *IEICE Trans. Fundamentals*, vol. E92-A, no. 12, pp. 3394–3397, December 2009.
 - [30] G. Kaddoum, F. Gagnon, P. Charge, and D. Roviras, “A generalized BER prediction method for differential chaos shift keying system through different communication channels,” *Wireless Personal Communications*, vol. 64, no. 2, pp. 425–437, 2012.
 - [31] G. Kaddoum, J. Olivain, G. Beaufort Samson, P. Giard, and F. Gagnon, “Implementation of a differential chaos shift keying communication system in gnu radio,” *Proc. ISWCS, 2012*, pp. 934–938, IEEE, 2012.
 - [32] H.G. Schuster and W. Just, *Deterministic chaos: an introduction*, John Wiley & Sons, 2006.